CLAIMS

What is claimed is:

1. A method comprising:

transmitting a first request from a source entity to a trusted arbitrator, the first request relating at least in part to establishing a secure connection between the source entity and a target entity;

establishing a secure connection between the source entity and the trusted arbitrator using a first encryption scheme in response to the first request;

transmitting a second request from a connection entity to the trusted arbitrator;

transmitting a first response from the trusted arbitrator to the connection entity in response to the second request, the first response being associated at least in part with the first request; and

establishing a secure connection between the trusted arbitrator and the connection entity using a second encryption scheme in response to the first response.

2. The method according to claim 1, wherein the trusted arbitrator authenticates with the source entity before the secure connection using the first encryption scheme is established.

3. The method according to claim 2, wherein the trusted arbitrator supports multiple authentication schemes and determines, before source entity is authenticated, whether a desired authentication scheme used by the source entity is supported.

4. The method according to claim 1, wherein the connection entity authenticates with the trusted arbitrator before the secure connection using the second encryption scheme is established.

5. The method according to claim 1, wherein at least one among the second request and the first response conforms at least substantially to a Hypertext Transfer Protocol.

6. The method according to claim 1, wherein at least one among the first and second requests is directed to a Uniform Resource Locator associated with the trusted arbitrator.

7. The method according to claim 1, wherein during at least a part of a period between a time of the transmitting of the first request and a time of the transmitting of the first response, the first request is stored in an area associated with the connection entity in the trusted arbitrator.

8. The method according to claim 1, wherein if the connection entity does not receive the first response within a predetermined period of a time of the transmitting of the second request, the transmitting of the second request is repeated.

9. A computer readable medium including computer readable instructions encoded thereon for:

transmitting a first request from a source entity to a trusted arbitrator, the first request relating at least in part to a target entity;

establishing a secure connection between the source entity and the trusted arbitrator using a first encryption scheme in response to the first request;

transmitting a second request from a connection entity to the trusted arbitrator;

transmitting a first response from the trusted arbitrator to the connection entity in response to the second request, the first response being associated at least in part with the first request; and

establishing a secure connection between the trusted arbitrator and the connection entity using a second encryption scheme in response to the first.

10. The computer readable medium of claim 9, further comprising computer readable instruction encoded thereon for authenticating the source entity before the secure connection using the first encryption scheme is established.

11. The computer readable medium of claim 10, wherein the trusted arbitrator supports multiple authentication schemes and determines, before the source entity is authenticated, whether a desired authentication scheme used by the source entity is supported.

12. The computer readable medium of claim 9, further comprising computer readable instruction encoded thereon for authenticating the trusted arbitrator before transmitting the first response.

13. The computer readable medium of claim 9, wherein at least one among the second request and the first response conforms at least substantially to a Hypertext Transfer Protocol.

14. The computer readable medium of claim 9, wherein at least one among the first and second requests is directed to a Uniform Resource Locator associated with the trusted arbitrator.

15. The computer readable medium of claim 9, wherein during at least a part of a period between a time of the transmitting of the first request and a time of the transmitting of the first response, the first request is stored in an area associated with the connection entity in the trusted arbitrator.

16. The computer readable medium of claim 9, wherein if the connection entity does not receive the first response within a predetermined period of a time of the transmitting of the second request, the transmitting of the second request is repeated.

17. A system in a computer network having a target entity, a connection entity coupled to the target entity, and an access control mechanism coupled to the connection entity, the system comprising:

a trusted arbitrator coupled to the access control mechanism; and

a source entity coupled to the trusted arbitrator, wherein

the trusted arbitrator receives a first request for establishing a secure connection from the source entity, the first request relating at least in part to the target entity,

in response to the first request, a secure connection is established between the source entity and the trusted arbitrator using a first encryption scheme,

the connection entity transmits a second request to the trusted arbitrator,

in response to the second request, the trusted arbitrator transmits a first response to the connection entity, the first response being associated at least in part with the first request, and

in response to the first response, a secure connection between the trusted arbitrator and the computer network is established using a second encryption scheme.

18. The system according to claim 17, wherein the secure connection between the trusted arbitrator and the computer network is established between the trusted arbitrator and the connection entity.

19. The system according to claim 17, wherein the secure connection between the trusted arbitrator and the computer network is established between the trusted arbitrator and the target entity.

20. The system according to claim 17, wherein the trusted arbitrator authenticates with the source entity before the secure connection using the first encryption scheme is established.

21. The system according to claim 20, wherein the trusted arbitrator authenticates the source entity by verifying identification information sent by the source entity.

22. The system according to claim 20, wherein the trusted arbitrator supports multiple authentication schemes and determines, before authenticating the source entity, whether a desired authentication scheme used by the source entity is supported.

23. The system according to claim 17, wherein an entity inside of the computer network authenticates with the trusted arbitrator before the secure connection using the second encryption scheme is established.

24. The system according to claim 23, wherein the trusted arbitrator supports multiple authentication schemes and determines, before being authenticated, whether a desired authentication scheme used by the computer network is supported.

25. The system according to claim 17, wherein the first request is a query that conforms at least substantially to a Hypertext Transfer Protocol, and the first response is a response that conforms at least substantially to a Hypertext Transfer Protocol.

26. The system according to claim 17, wherein the access control mechanism is a firewall.

27. The system according to claim 17, wherein the access control mechanism is a proxy server.

28. The system according to claim 17, wherein the access control mechanism is coupled to the trusted arbitrator at least in part through the Internet.

29. The system according to claim 17, wherein the remote entity is coupled to the trusted arbitrator at least in part through the Internet.

30. The system according to claim 17, wherein at least one among the first and second requests are directed to a Uniform Resource Locator associated with the trusted arbitrator.

31. The system according to claim 17, wherein during at least a part of a period between a time of the sending of the first request and a time of the sending of the first response, the trusted arbitrator stores the first request in an area associated with the connection entity.

32. The system according to claim 17, wherein if the connection entity does not receive the first response within a predetermined period of a time of the sending of the second request, the sending of the second request is repeated.

33. The system according to claim 17, wherein before a time of sending the first response, the trusted arbitrator sends a notice to the connection entity, said notice being in response to the first request.

34. The system according to claim 17, wherein the connection entity forwards at least a portion of the first request to the target entity.

35. A system for establishing a secure connection comprising:

a computer network employing an encryption scheme, said computer network including a target entity, a connection entity coupled to the target entity, and an access control mechanism coupled to the connection entity;

a trusted arbitrator coupled to the access control mechanism; and

a source entity coupled to the trusted arbitrator, the source entity employing the same encryption scheme, wherein the trusted arbitrator authenticates with the source entity and the connection entity,

the trusted arbitrator receives a first request for establishing a secure connection from the source entity, the first request relating at least in part to the target entity,

the connection entity transmits a second request to the trusted arbitrator,

in response to the second request, the trusted arbitrator transmits a first response to the connection entity, the first response being associated at least in part with the first request, and

in response to the first response, a secure connection between the source entity and the computer network is established using the encryption scheme.

36. The system according to claim 35, wherein the secure connection between the source entity and the computer network is established between the source entity and the connection entity.

37. The system according to claim 35, wherein the secure connection between the source entity and the computer network is established between the source entity and the target entity.